FINGERTEC

i-Kiosk 100 Plus

Premier Color Multimedia Fingerprint Time Attendance & Access Control System

FING@RTEC

U S E R   G U I D E

i-Kiosk 100 Plus
Premier Color Multimedia Fingerprint Time Attendance & Access Control System

DISCLAIMER

No person should rely on the contents of this publication without first obtaining advice from a qualified professional person. The company expressly disclaims all and any liability and responsibility to any reader or user of this book, in respect of anything, and of the consequences of anything, done by any such person in reliance, whether wholly or partially, upon the whole or any part of the contents of this book.

FINGERTEC WORLDWIDE LTD

For enquiries on technical matters, please forward the email to
support@fingertec.com

CONTENTS

① GETTING STARTED

i-Kiosk 100 Plus

IMPORTANT SAFEGUARDS

INSTALLATION LOCATION

Do not install readers in areas which are exposed to bright sunlight or rain, as the fingerprint readers are not designed to work in those areas. Bright light will interfere with reading of the sensor and fingerprint readers are not waterproof or vandal proof. It is recommended to protect your fingerprint readers with enclosure.

Go to **http://accessory.fingertec.com** to view the enclosure and other accessories.

USE OF SENSOR

Do not abuse the fingerprint sensor by scratching the surface, contacting the sensor's surface with heat, pressing hard during placement of fingerprint for verification. Clean the sensor occasionally with cellophane tape to maintain the performance of the sensor.

INTRODUCTION TO READER

FingerTec® introduces the i-Kiosk series, the multi-faceted touch screen biometric equipment that will change the way you look at fingerprint verification technology. Aside from offering the expedience of multiple verification methods, it is user-friendly and is furnished with SGVA high color resolution.

Developed with the advanced Embedded LINUX operation system, the FingerTec® i-Kiosk 100 Plus does keep up with the latest technology as it adds WiFi and GPRS functionality for a faster, seamless, and more stable real-time transfer of attendance data. It allows storage of 100,000 transactions at a time and a maximum of 3,000 fingerprint templates. It is also suitably equipped with 8 function keys and a touch screen control panel with integrated camera display for easier and quicker navigation.

FingerTec® i-Kiosk 100 Plus is a smart choice for time attendance and door access system for its versatility. There's no need to worry if a fingerprint cannot be verified immediately – access can be had by proximity card and password identification too. The wide-screen 8-inch LCD for vivid colorful display provides enhanced user experience as it can be used for MP3 music and short movie playback.

With all the outstanding features it can offer, there is no doubt the i-Kiosk 100 Plus is the perfect solution to a company's biometric time attendance and door access requirement.

SPECIFICATION

Display area (inch)	8.0 TFT screen
Color resolution	65k
Surface finishing	Acrylonitrile Butadiene Styrene (ABS)
Functions	Time attendance and door access control system
FP storage	3000
Transaction log	120000
Connection available	TCP/IP, RS232, RS485, USB flash disk (pen drive), USB host-client, Wiegand 26-bits input and output, WiFi / GPRS
Card reader	RFID card reader
Card capacity	65534
Sensor	Optical scanner with silicon coating
Multimedia functions	Short message display, Short movies playback, MP3 playback
Software	***Language available*** English, Arabic, Indonesian, Spanish, Thai, Portuguese, Chinese, French, Russian, Farsi, Italian, Vietnamese, German, Italian

COMPLETE PACKAGE

Fingerprint Reader

RS232 cable

Screws

DC 12V Power Adapter

Key

Li-icon battery

RFID Card (5pcs)

Screwdriver

USB Flash Disk *(Optional)*

Software CD

3 Pin Plug

2 Pin Plug

MATERIALS PROVIDED

- Quick Start Guide
- Hardware User Manual
- Software User Manual
- Video Guide for Hardware
- Video Guide for Software
- Sample of Enrollment Form

BASIC FEATURES

L.E.D DISPLAY
The L.E.D display has two lights.
Green - The reader is in standby mode or to indicate that user has been successfully verified.
Red - To indicate that user verification has failed

COLOR LCD
Screen that displays instruction and status of reader. This is a touch screen panel. You can press the screen to do settings without using keypads.

FUNCTION KEYS
Shortcut keys to enter specific command to reader

ANTENNA
To send/receive signal of WiFi or GPRS

RFID CARD
RFID card induction area

NAVIGATION KEYS
To navigate and to input command to reader

OPTICAL SCANNER
For user to place finger for enrollment or verification

KEYPADS
Keys from 0-9, alphabets Power on/off button, Escape/Cancel button, Menu/Enter button, backspace button, asterisk (*) button, hash (#) button

SPEAKER
To prompt user with result of verification and information

Number and Alphabet keys

Escape

Menu/Enter

Backspace

Asterisk

Hash

Power On/Off

2 USING THE FINGERPRINT READER

USING THE FINGERPRINT READER

This chapter will guide on how to use the fingerprint reader effectively. To get a good reading every time, initial fingerprint enrollment must be done properly.

Center points

FingerTec® i-Kiosk 100 Plus reader provides 4 types of enrollment method:

1 FINGERPRINT ENROLLMENT
User enrolls his fingerprint template into a reader and the template will be used for future verifications.

2 PASSWORD ENROLLMENT
For user who has difficulty to enroll fingerprint due to poor fingerprint quality, enrollment of password is recommended. Password enrollment is also suitable for visitors and temporary workers.

3 FINGERPRINT AND PASSWORD ENROLLMENT
Under this option, a user can enroll both fingerprint and password at the same time. The user can either use fingerprint or password to report attendance or to gain access.
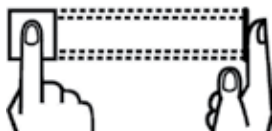
4 RFID CARD ENROLLMENT
Please refer to Chapter 3 for RFID Card Function.

TIPS FOR BEST FINGERPRINT ENROLLMENT

What you should DO

Place finger flat on the fingerprint sensor. Make sure the finger's midpoint is placed at the center of the fingerprint sensor.
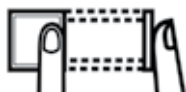
What you should NOT do

UPRIGHT

ASKEW

OFF CENTER

PART

1 USE INDEX FINGER

Index finger is smaller than thumb and it can be comfortably placed on the sensor. The use of thumb is not recommended because the center points might not be placed properly on the sensor, hence cannot be read by the sensor.

2 MAKE SURE THE FINGER IS NOT WET, TOO DRY, INJURED OR DIRTY

The finger needs to be slightly moist to enable the sensor to read the minutiae points on the fingerprint.

3 PLACE THE CENTER POINTS OF YOUR FINGER AT THE CENTER OF THE SENSOR

The center points of a finger is an area where there is a swirl and the center points must be properly placed on the sensor during enrollment.

4 DON'T PRESS HARD AT THE SENSOR, JUST PLACE YOUR FINGER ON THE SENSOR

The sensor is reading minutiae points of your finger and placing a finger properly on the sensor will prompt the sensor to read those points. Pressing your finger hard on the sensor is not necessary.

5. DON'T DO ENROLLMENT UNDER BRIGHT LIGHT OR DIRECT SUNLIGHT

It is important to note that bright light or sunlight could interfere with reading of the sensor. Avoid placing the reader under direct sunlight or bright light to avoid difficulty in enrollment and future verification.

INITIAL SET UP OF
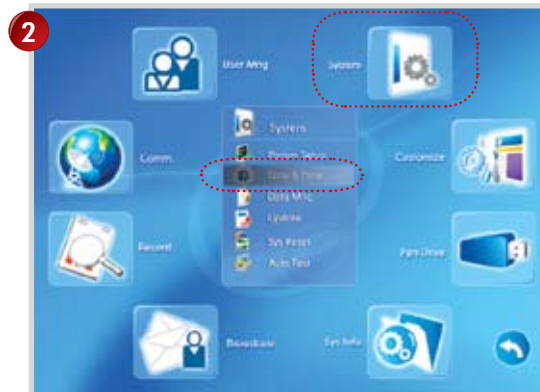## THE FINGERPRINT READER

DATE / TIME ADJUSTMENT

When first installing a fingerprint reader, it is important to set the correct date and time.

Follow the steps shown to access the Date/Time adjustment menu:

Select the Menu button.

Select System followed by Date & Time.

The arrow buttons control the movement of the cursor.
Enter time value by using the numeric keypad.
Select Done to save settings.

DLST stands for Daylight Saving Time.
Please enter the date and time in the given column to use this feature.

DLST: Enter date and time for daylight saving starts
Standard: Enter date and time to return to standard

Select OK to confirm.

Select the return arrow to go to the Main Menu.

ENROLLMENT

To assist in fingerprint enrollment, please use the form provided. The administrator can keep track of the enrollment detail. You can design your own form to suit to your company's requirements.

User Enrollment Template Form for Reader   Reader ID: _____

No.	User ID	Employee No.	Name	Department	IC No.	No. of Fingers Enrolled	Date Registered	Note	Signature

SAMPLE

ENROLLMENT OF SUPERVISOR / ADMINISTRATOR

Once the fingerprint reader is switched on, a display on screen will appear. Enroll a supervisor or an administrator, the in-charge person to administer the fingerprint templates and the transaction data in the reader. Choose trustworthy people for this particular role.

Select the Menu button.
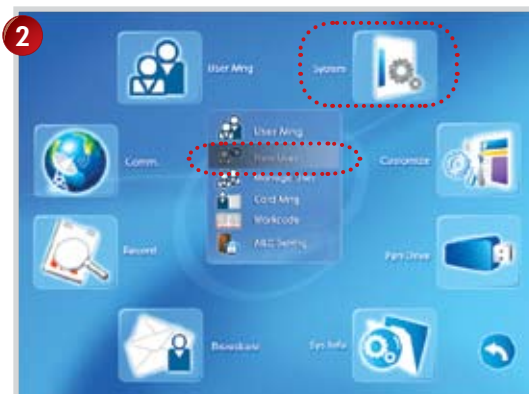
The page will automatically turn to User Management.
Select New User.

Enter the user ID in the ID No. column using the numeric keypad,
for example 1.

Use ▶ to go to Authority field to change it to Admin.

Select Enroll Fingerprint to start fingerprint enrollment.

Press finger firmly on the optical scanner to enroll fingerprint.

The enrolled fingerprint image will be displayed on the screen.
Place the same finger on the scanner for another 2 times.

This screen will be displayed after a successful enrollment.
end the enrollment process.

The screen will return to the previous page. The FP num =1, Select Done to
indicates that a fingerprint has been enrolled for this user ID.
Select Done to save settings.

Select OK to confirm.

You can repeat the above steps to enroll another user.
Select Done to end enrollment.

Select the return arrow to go back to the main menu.

ENROLLMENT OF NORMAL USER

A normal user is only allowed to use the reader for identity verification, and he does not have any other authorities to access the system. To add a normal user, follow the steps shown.
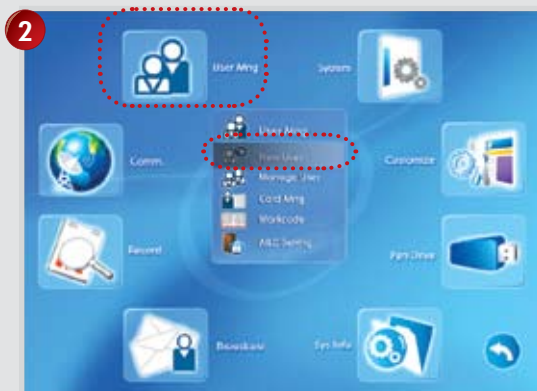
Select the Menu button.

The page will automatically turn to User Management. Select New User.

Enter the user ID in the ID no. field using the numeric keypad for example 2.

Go to the Authority field and use ▶ to change it to User.

Select Enroll Fingerprint to start enrollment.

Press finger firmly on the optical scanner to enroll fingerprint

The enrolled fingerprint image will be displayed on the screen.
Place the same finger on the scanner for another 2 times.

8 Enroll Sucess!

DONE

BACK

This screen will be displayed after a successful enrollment.
Select Done to end the enrollment process.

9 User Registration

ID NO   2

Name

FP

Pwd   Enroll Password

Authority   User

Card   Enroll card

Capture Mode   Use Globe Setting

Photo   Enroll Photo   Preview

DONE

BACK

The screen will return to the previous page. The FP num =1,
indicates that a fingerprint has been enrolled for this user ID.
Select Done to save settings.

10 User Registration

ID NO   2

Name

FP

Pwd   Enroll

Authority   User

Card   Enroll card

Capture Mode   Use Globe Setting

Photo   Enroll Photo   Preview

DONE

BACK

Select OK to confirm.

11 User Registration

ID NO   3

Name

FP   Enroll Fingerprint

Pwd   Enroll Password

Authority   User

Card   Enroll card

Capture Mode   Use Globe Setting

Photo   Enroll Photo   Preview

DONE

BACK

Repeat the above steps to enroll another user.
Select Done to end enrollment process.

Select the arrow to return to the main menu.

To enroll more users, repeat the steps above.

FINGERPRINT VERIFICATION

The reader supports 2 types of fingerprint verification method. User can choose either method to verify his fingerprint at the reader.

• 1 to Many (1:N) fingerprint matching

• 1 to 1 (1:1) fingerprint matching

1 TO MANY (1:N) FINGERPRINT MATCHING

Place the enrolled fingerprint on the fingerprint sensor.
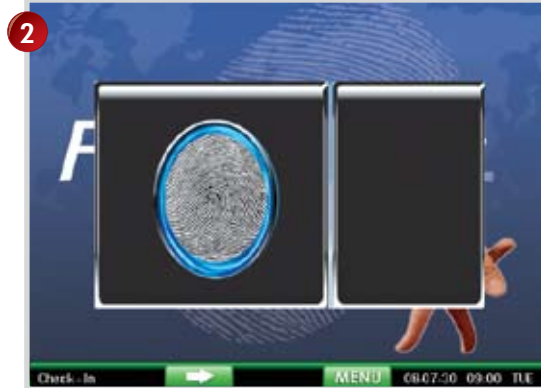
Wait a second before removing the finger from the fingerprint sensor.

The reader will verify user, display his user ID and prompt "Thank you".

If verification failed, the reader will prompt "Please try again."

1 TO 1 (1:1) FINGERPRINT MATCHING

Enter the user ID by using the numeric keypad.

Place the enrolled finger on the fingerprint sensor.
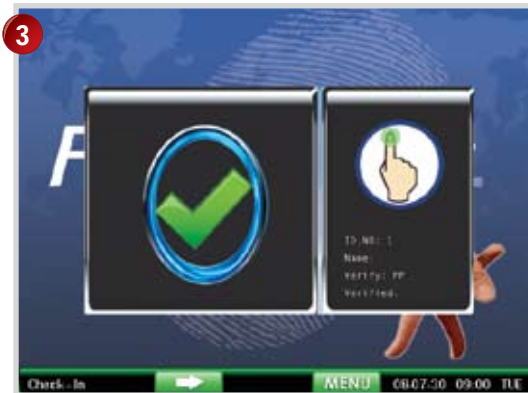
The reader will verify user, display his user ID and prompt
"Thank you.".
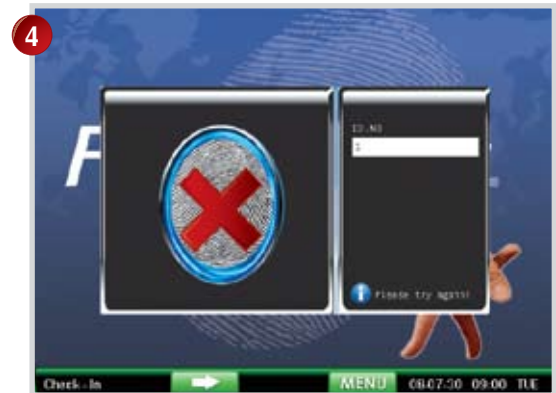
If verification failed, the reader will prompt "Please try again."

PASSWORD ENROLLMENT

For user who cannot enroll his fingerprint, he can choose to use passwords.

Follow the steps below:

Select the Menu button.
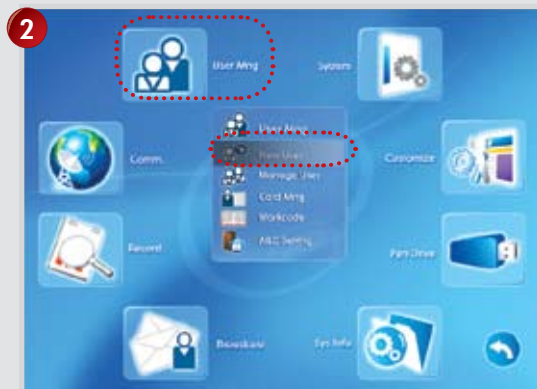
Select New User to start.

Enter user ID into the ID No. column using the numeric keypad for example 3.

Go to the Authority field and use the ▶ to change to User.

Select Enroll Password.

Enter password in the column, a maximum of 8-digit.

Select ▼ to go to the next field.
Re-enter password to confirm. Press Done to save settings.

There will be a key icon on the screen to indicate that this user ID
has been enrolled with password. Select Done to save settings.

Select OK to confirm.

Repeat the above steps to enroll new user.
Select DONE to end process.

Select the arrow to return to the main menu.

PASSWORD VERIFICATION

User with password enrollment can always use password to report attendance or gain access from the readers.

Enter user ID.

Select OK button.

Enter password using numeric keypad.

Press OK to confirm password.
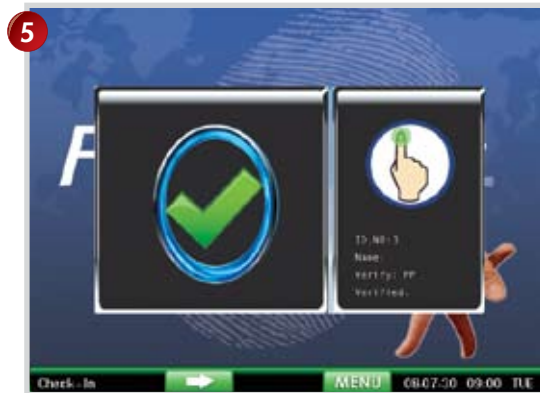
The reader will verify user, display user ID and prompt "Thank you".

If verification failed, the reader will prompt, "Please try again".

DELETING USERS

The system allows deletion of user from the system. This is important as employees come and go. Therefore, for those who had left the company, their fingerprint templates or records must be deleted from the system to avoid any misuse of the system. Only an administrator or a supervisor has the rights to delete user.

Follow the steps shown to delete users.
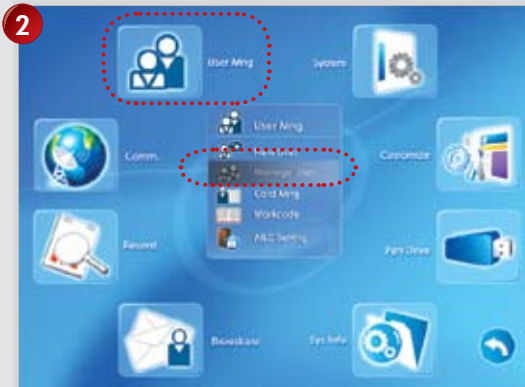
Select Menu button.

Select Manage User.
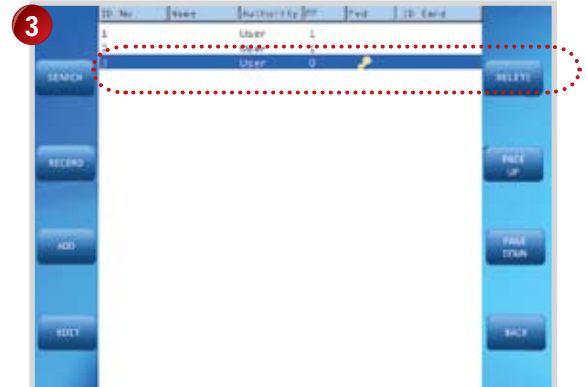
All users will be displayed on the screen. Select the User ID you wish to delete. Select Delete to proceed.

Select Delete User.

Select OK to confirm.
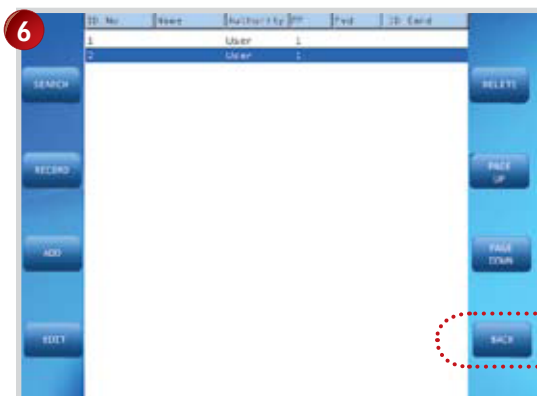
The screen will refresh and user ID will be deleted from records. Select Back to return to the previous page.

Select the arrow to return to the main menu.

③ RFID CARD FUNCTION

The reader supports enrollment of RFID Card. User can report time attendance and gain access by using RFID card. At the same time, users with fingerprint or password enrollment can add RFID card as well.

Each RFID card has a unique ID. During enrollment this Card ID will be read from the RFID card and stored in the reader. During verification the reader will match the ID in the card to the ID stored in the reader.

ENROLLMENT OF RFID CARD

Each RFID card user must register his RFID card to the reader.

To enroll user with RFID card, follow the steps shown:

Select the Menu button.

Select the New User button.

Enter user ID using the numeric keypad for example 4.

Select ▶ to change Authority field to user.

Select Enroll Card to start enrollment of RFID card.
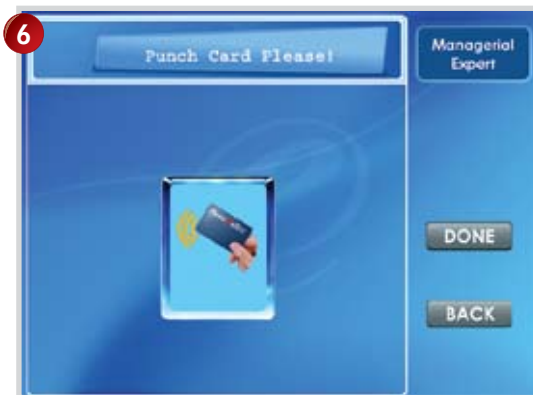
Wave RFID card at the induction area.
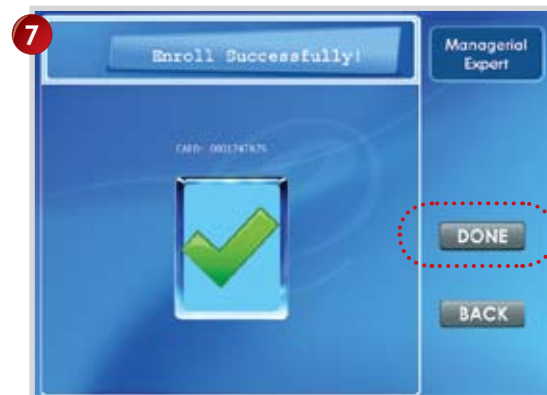
The reader will capture RFID Card ID and display it on screen. Select Done to end process.

The card icon will appear to indicate that this user ID has been enrolled with RFID card. Select Done to save settings.

Select OK to confirm.

Repeat the steps above to enroll new card user.
Select Back to return to the previous page.

Select the return arrow to go back to the main menu.

ADD RFID CARD TO EXISTING FINGERPRINT USERS

Existing fingerprint users can choose to use RFID card as a backup verification method. These users can either verified using fingerprint or RFID card. To add RFID card to existing fingerprint users, please follow the steps below:

Select the Menu button.
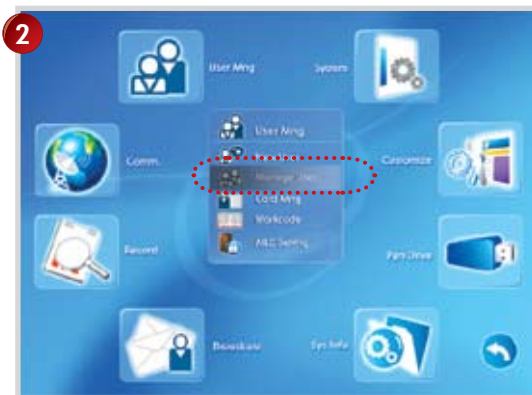
Select Manage User.
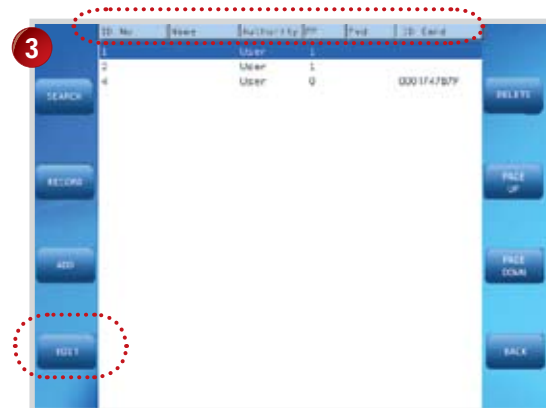
Select ▲▼ to choose the user ID to add RFID card for example user ID 1. Select Edit button.

Select Enroll Card to start RFID card enrollment.

Wave RFID card at the induction area.

RFID card will be read and card number displayed on the screen. Select Done to save settings.

There is a card icon indicates that user has been enrolled with RFID card. Select Done to save settings.
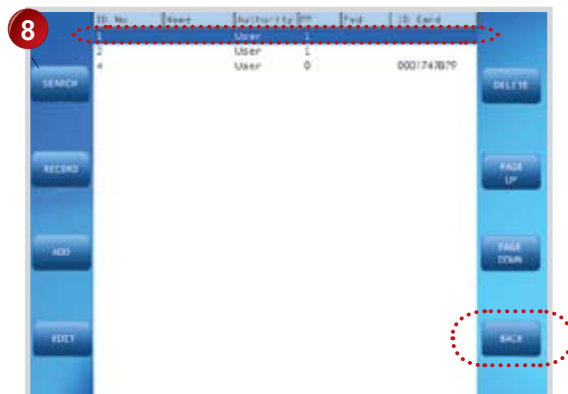
The screen will refresh and the RFID card numbers will appear on User ID 1. Select Back to return to the previous page.

Select the return arrow to go back to the main menu.

VERIFICATION WITH RFID CARD

RFID card user can do verification at the reader by the following combinations:

To enable this operation, configure option Card Only in Advance Option to Yes.

Wave RFID card at the induction area.
The reader will read the RFID card to verify it.

The RFID card number and User ID will be displayed on screen, and reader will prompt, "Thank you".

If verification failed, the screen will show RFID card number and message "Not enrolled".

4 ACCESS OPTIONS

BRIEF INTRODUCTION TO ACCESS OPTIONS

Access option function setting is the settings of user's accessibility to certain doors. It is known as Time Zone. A combination of time zones is known as Group Time Zone. There are a total of 50 time zones available in the reader. Below are some examples of Time Zone configurations and combinations of Time Zones.

Time zone	1
SUN	09:00-18:00
MON	09:00-18:00
TUE	09:00-18:00
WED	09:00-18:00
THU	09:00-18:00
FRI	09:00-18:00
SAT	09:00-18:00

Table 1.1 Time Zone 1

TIME ZONE 1

CONSTANT ACCESS TIME FOR A PERIOD OF ONE WEEK.

Table 1.1 is showing the time zone 1 detailed schedule where users are only allowed access from 9am to 6pm from Monday to Sunday.

Time zone	2	3
SUN	23:59-00:00	23:59-00:00
MON	08:00-12:00	14:00-18:00
TUE	08:00-12:00	14:00-18:00
WED	08:00-12:00	14:00-18:00
THU	08:00-12:00	14:00-18:00
FRI	08:00-12:00	14:00-18:00
SAT	23:59-00:00	23:59-00:00

Table 1.2 Time Zones 2 & 3

TIME ZONE 2

VARIATION IN ACCESS FOR A PERIOD OF ONE WEEK.

Table 1.2 is showing the time zone 2 where users are allowed access from 8am to 12pm from Monday to Friday but denied access on weekends.

TIME ZONE 3

VARIATION IN ACCESS FOR A PERIOD OF ONE WEEK.

Table 1.2 also is showing the time zone 3 where users are allowed access from 2pm to 6pm from Monday to Friday but denied access on weekends.

The Time Zone 2 and Time Zone 3 belongs to the same group of employee, therefore they can be grouped together in Group Time Zone, for example Group Time Zone 1.

There are a total of 5 Group Time Zones available for use.

Every new registered user belongs to Time Zone 1. Default grouping combination is Group 1 and default Group Time Zone 1.

Group time zone	Time zones
1	2 3
2	
3	
4	
5	

Table 1.3 Group Time Zones

Under a condition where Group 1 and Time Zone 1 are in factory default status, new registered user defaults in unlocking status. If the grouping of that user does not include in grouping combination setting, then user can only record time attendance but cannot unlock the door.

Access option has 6 main functions

- **TIME ZONE SETTING**
  To define time zone 1 to 50.

- **HOLIDAY SETTINGS**
  To define time zone for holiday.

- **GROUP TIME ZONES SETTINGS**
  To define group time zones, a group
  can support up to 3 different time zones.

- **UNLOCK COMBINATION SETTINGS**
  To define different time zone combinations,
  and each combination is composed of
  different groups.

- **ACCESS CONTROL PARAMETERS**
  To define lock/unlock parameters

- **DURESS ALARM PARAMETERS**
  To define duress alarm parameters.

FUNCTION DESCRIPTION DEFINITION OF TIME ZONE

TIME ZONE
Range of time specified for access options. The system can define a maximum of 50 time zones. Each user can set a maximum of 3 times zones.

TIME REGION
A certain period of time with a format of HH:MM–HH:MM, operates in 24-hr format and accurate to the minutes. For each time zones, 7 time regions can be set.

ALL DAY ACCESS
00:00 to 23:59, reader allows user to access anytime in a day.

FORBIDDEN TIME ZONE
23:59 to 00:00, reader blocks users to access anytime in a day.

All new enrolled users are automatically assigned to Time Zone 1. It is recommended not to change any settings in Time Zone 1.

For example,
Users are allowed to access from 8:00 am – 12:00pm during working hours from Monday to Friday. Saturdays and Sundays are off days and users are not allowed any entry.

Follow the steps to configure time zones.

Select A/C Settings.

Select Time Zone Settings.

Select Add to add a new time zone.

Press arrow key to move around the columns. Insert the time in the columns to define time zone. Select Done to save settings.

Press OK to save settings.

Select Back to return to the previous menu.

A new time zone is displayed on screen.
Select Back to return to the previous menu.
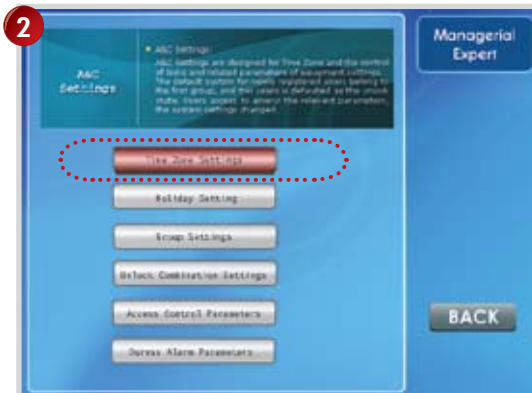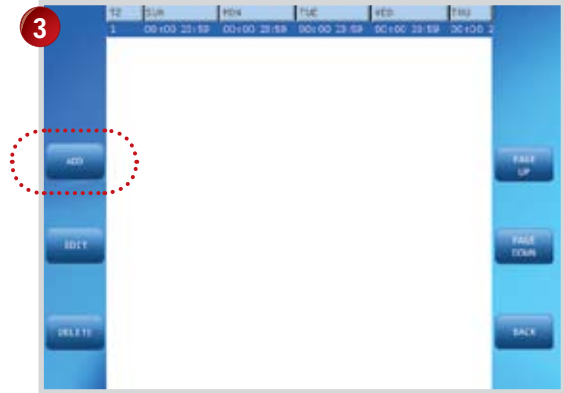
The configured time zone is saved and reader is allowed to set the next time zone. A total of 50 time zone is available and each user can use up to 3 time zones.

After time zones settings are configured, these time zones shall be included in the Group Time Zones for the configuration to take effects.

DEFINITION OF GROUPING FUNCTION

Grouping function can segregate users into group and combine different groups into different unlocking combinations. The function provides convenience to grouping management of Access Options. The grouping function can combine as many unlocking combinations as possible from the five groups. New registered user default belongs to Group 1 but the users in Group 1 can be relocated into another group.

Follow the steps to configure group time zone,
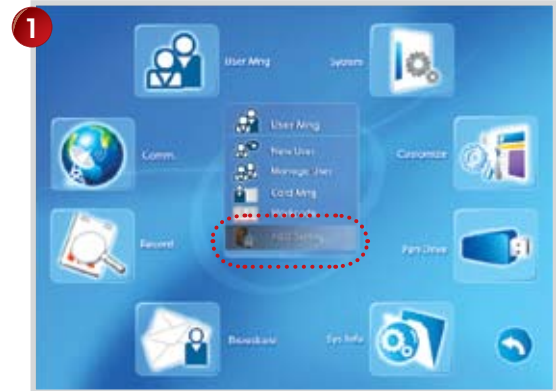
Select A&C Setting.
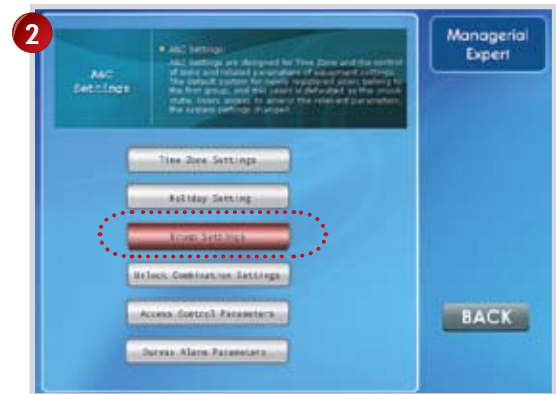
Select Group Settings.
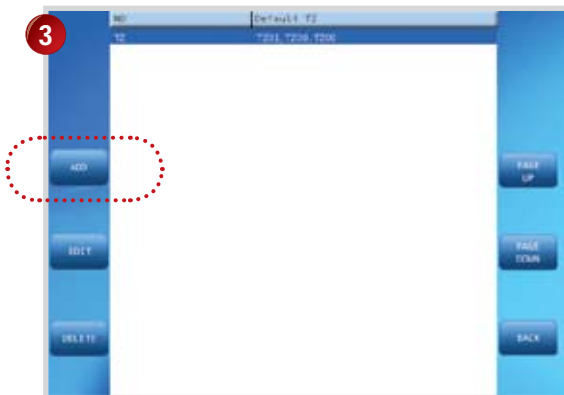
Select Add to add in a new group time zone.

Insert the corresponding information into the columns as shown.

NO: Group time zone

Holiday: Invalid (to block user during holiday)

TZ1 / TZ2 / TZ3: Time zone to be followed in this gruop; maximum 3 different time zones
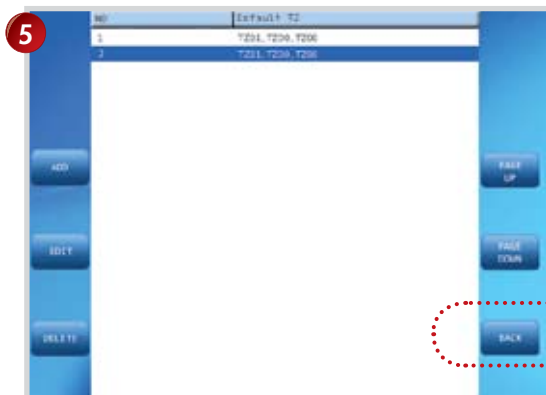
A new group time zone is displayed on screen.
Select Back to return to the previous menu.

DEFINITION OF
USER ACCESS SETTINGS

User Access Options is to process correlative setting according to user's requirements.

ENTER ACCESS OPTIONS MENU TO CHECK USER'S ACCESS OPTIONS STATUS

User Access Options include user grouping setting, use group time zone and user time zone.

GROUPING

Divides registered users into several groups making them managable.

USE GROUP TIME ZONE

Whether the user uses default time zone of the belonged group.

USER TIME ZONE

For user to set user's unlocking time, and select number of time zone already being set.

FOR EXAMPLE,

User ID 00001 is assigned to Group Time Zone 2. Follow the steps to assign user into group time zone.

At the main menu, select Manage User.
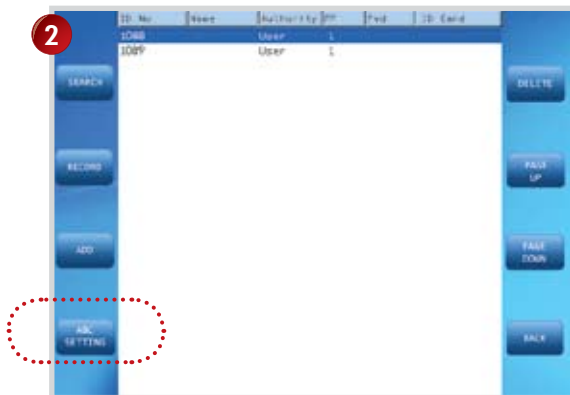
Select the user ID to assign time zone to for example 1888.
Select A&C settings.

Insert 2 into the column Group no. Select Done to save settings.
Now User ID 1888 is assigned into Group Time Zone 2, and this
group controls his accessibility.

DEFINITION OF
HOLIDAY SETTINGS

User access time can control reader during holiday.
The access time zone might vary during holiday and
the time zone for holiday can be preset.

During configuration of the time zone for holiday, the
time range for the time zone is time to block users to
gain access.

EXAMPLE,

Users are allowed to access during holiday from 8:00
to 12:00. Therefore, you must configure in time zone
as below

$$13:00 - 23:59$$

This is the time range to block users to gain access from
the reader. Please take note, time zone for holiday has
a different concept than the normal time zone.

Select A&C Settings.

EXAMPLE OF SETTINGS

Select a public holiday for example 1st May. The reader is set to disallow any access during holiday. Follow the steps shown to configure holiday settings.
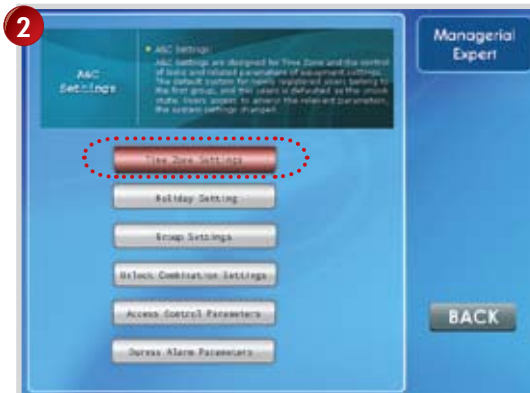
Select Time Zone Settings.
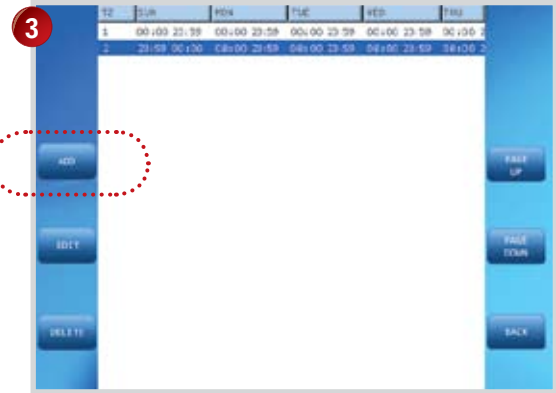
Select ADD to add a new time zone.

Now configure the time to block user to access to certain time zones.
To block access for the entire day, you will need to configure
00:00 – 23:59.
Repeat the configuration for the whole week.
Select Done when finish.

Select OK to save settings.
Select Back to return to the previous menu.

Select Holiday Settings.
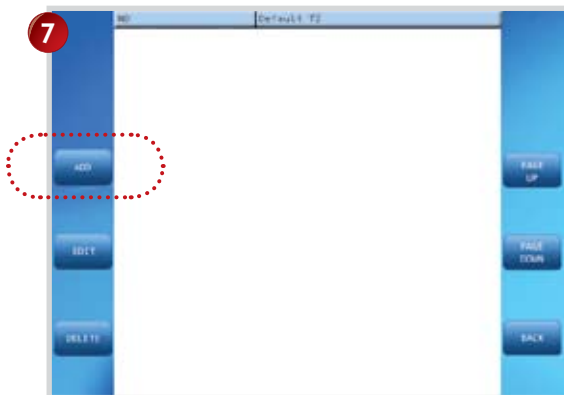
Select ADD to add in a new holiday.
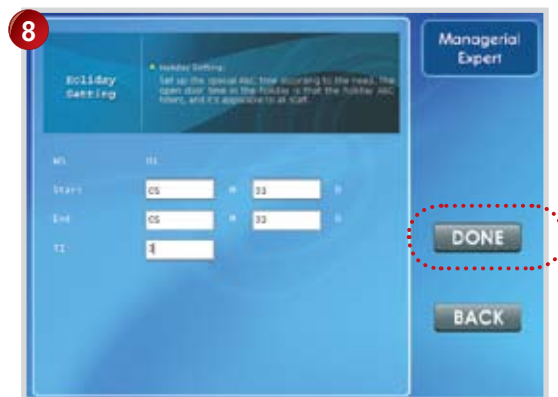
Assign the starting and ending date of the holiday.
Insert the time zone to block user to access.
Select Done to save settings.
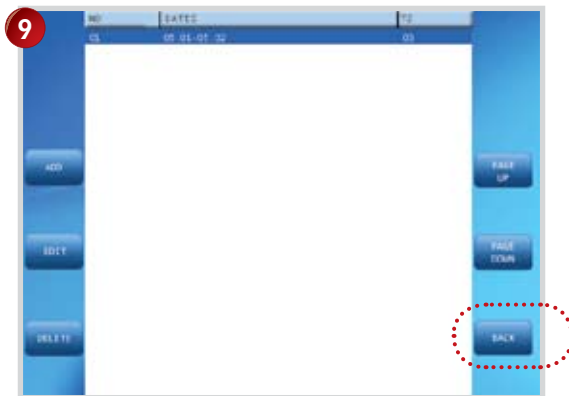
Select Back to return to the main menu.

USER UNLOCK COMBINATION SETTINGS

The reader can support unlock combination to control user accessibility.

When unlock combination is activated, reader will request verification from multiple users from different group time zone for example 3 users from 3 different group time zone must verify at the reader.

Each user must have a valid time zone during the verification process.

The reader will not open door if:

1 – user's group time zone is not included in the combination.

2 – the time zone of user is invalid during verification process.
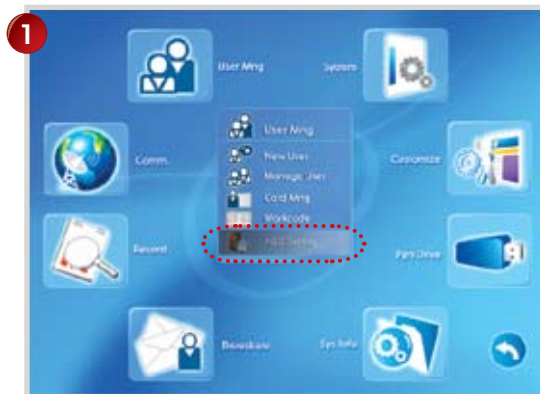
Select A&C Settings.
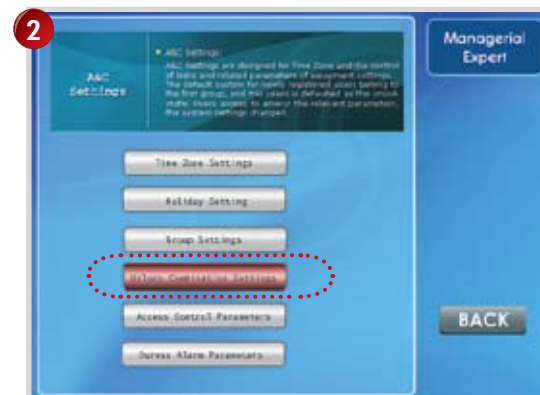
Select Unlock Combination Settings.
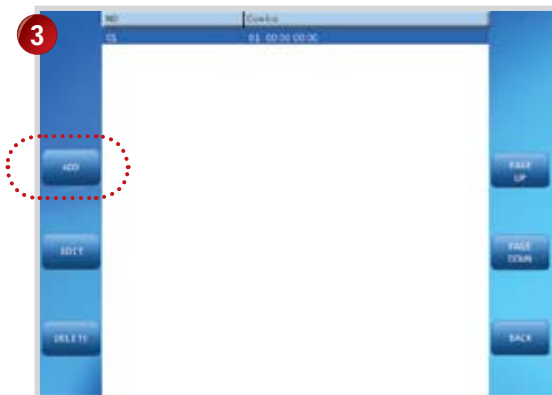
Select ADD to add a new unlock combination group. By default, all users are assigned into Combo 1, where it supports group time zone 1 only.

Insert the name of Combo, for example 2. Insert the group time zones to be included into this Combo. Maximum is 5 group time zones.
Select Done to save settings.

Select OK to confirm.
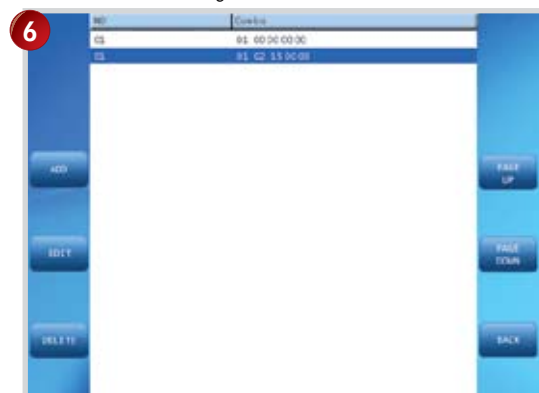
A new unlock combination group is displayed on screen.
You can assign users into the group by referring to User Access Settings.

ACCESS CONTROL PARAMETERS

This page allows administrator to configure accessibility of readers. There are total 8 options ready for configuration. Follow the steps to enter to access control parameters.

Select A&C settings.
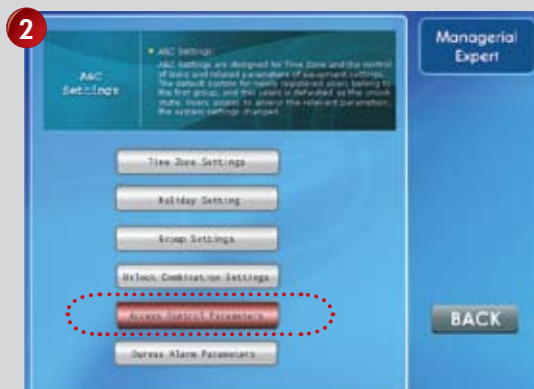
Select Access Control Parameters.
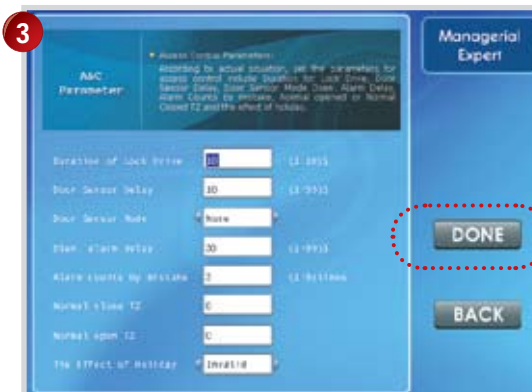
Select Done to save settings.

Options available and their functions

LOCK (1-10S)
To adjust the unlocking time after verification.

DSEN. DELAY (1-99S)
To delay door sensor from triggering alarm system when door is not closing. This function only works when a door sensor is attached to the reader.

DSEN MODE
To choose the type of door sensor attached to the reader. There are NO (normally opened) and NC (normally closed) available. Choose NONE if no door sensor is attached.

ALARM DELAY (1-99S)
To delay the reader from triggering alarm system.

ALARM COUNT (1-9 TIMES)
To adjust the maximum verification failures of users. When the maximum is reached, reader will trigger alarm system.

CLOSE TZ
Door is always locked during the predefined time period, so users cannot gain access after verification.

OPEN TZ
Door is always unlocked during the predefined time period, so users do not need to verify their identities but can gain access.

VALID HOLIDAYS
Choose Valid to enable the holiday settings. Choose Invalid to disable the holiday settings.

DURESS ALARM PARAMETERS

The fingerprint reader will trigger alarm system after a duress fingerprint is verified successfully. It is advisable

1

To use different fingers to do daily clocking mechanism and to trigger duress alarm

OR

2

To use different verification to do daily clocking mechanism and to trigger duress alarm.
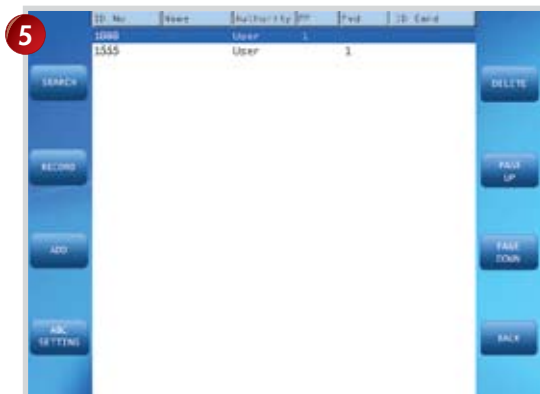
Select A&C settings.

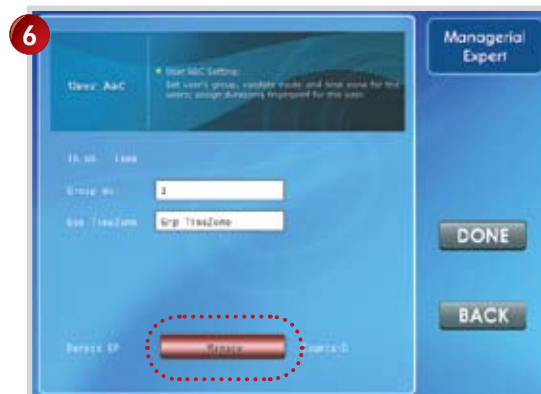Select Duress Alarm Parameters.
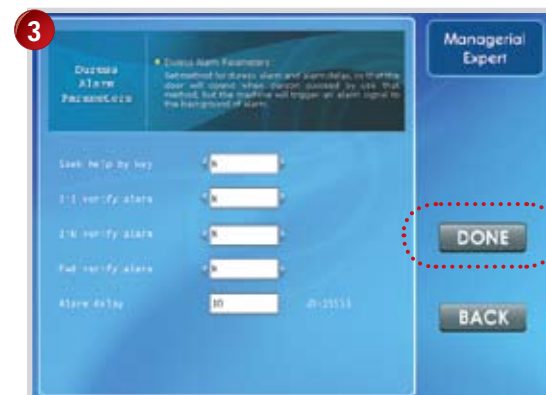
To define Duress Fingerprint. Select DONE to proceed.
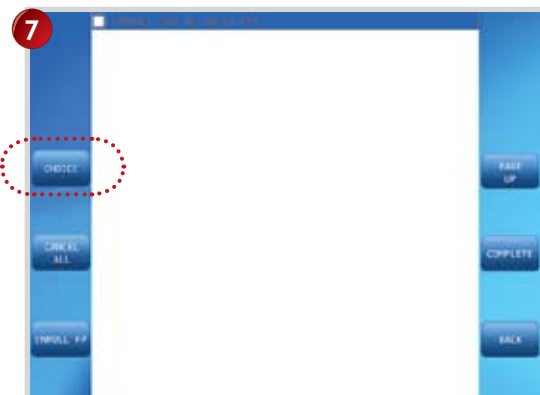

Select Manage User.

Select user ID to assign duress finger, for example user ID 1888.

Select Manage

Choose the fingerprint to be defined as duress finger by selecting "Choice".

Select Done to save settings.

Select OK to confirm.
Select Back to return to the previous menu.

OPTIONS AVAILABLE AND THEIR FUNCTIONS

If users would like to use the same fingerprint for daily clocking and to trigger duress alarm, administrator must enable either one of the following functions.

HELP KEY

Select [Yes] to enable. Hold the ▼ for 3 second followed by the fingerprint verification. Successful verification will trigger alarm system.

1:1 TRIG

Select [Yes] to enable. Enter user ID followed by fingerprint verification to trigger alarm system. During daily clocking mechanism, all users use 1:N fingerprint verification. All 1:1 fingerprint verification process will trigger alarm system.

1:N TRIG

Select [Yes] to enable. Place finger on scanner for fingerprint verification to trigger alarm system. During daily clocking mechanism, all users use 1:1 fingerprint verification. All 1:N fingerprint verification process will trigger alarm system.

PWD TRIG

Select [Yes] to enable. Enter user ID and password for verification to trigger alarm system. During daily clocking mechanism, all users use fingerprint verification. Any password verification process will trigger alarm system.

ALARM DELAY

To delay the reader to trigger alarm system after verification. If user would like to enroll another finger to trigger duress alarm, please disable all of the above option.

Please see the next page to learn on how to enroll/define a finger to trigger duress alarm.

5 MOST FREQUENTLY USED FUNCTIONS

There are 3 most frequently used functions in this reader:

• USB flash disk (pen drive)

• Work Codes

• Alarm

USB FLASH DISK (PEN DRIVE)

If a reader is installed remotely from a computer or encountering connection problems that are causing disruption of data download, user can transfer data via USB flash disk.

Plug in your USB flash disk and follow the steps shown below:

Select the Menu button.

Select the Pen Drive icon.

There are a total of 10 operations available to choose from.

Upload users: To upload users into reader.

Upload pictures: To upload pictures (for screen saver) into reader.

Upload users photo: To upload user photo into reader.

Upload SMS: To upload preset short messages into reader.

Upload flash: To upload flash into reader.

Download User: To download users into USB flash disk.

Download Attg: To download transaction logs into USB flash disk.

Download user photo: To download users' photo into USB flash disk.

Download SMS: To download short messages into USB flash disk.

Download capture photo: To download captured photo into USB flash disk.

WORK CODES

Work code feature is available in this fingerprint reader. The work code feature allows user to enter a predefined number after identity verification. User will enter a number being assigned after as work code to show purpose of their clocking data.
Table below is showing examples of work code function predefined by numbers.

Reasons	Work Code
Check In	00
Check out	01
OT start	04
Done	05
Sick Leave	10
Half Day Leave	12
Emergency Leave	11
Meeting Client	20
Outstation	21

These numbers are predefined by user in the software and they represent different reasons, such as "10" for sick leave, "11" for emergency leave. It is recommended to predefine all work codes using software. However, shall you choose to predefine work codes at the reader itself, follow these steps:

Select the Menu button.
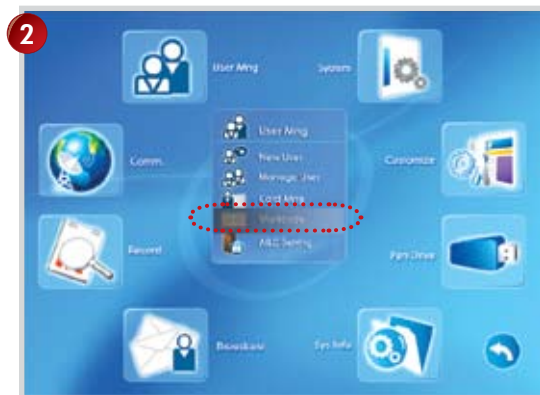
Select Workcode.
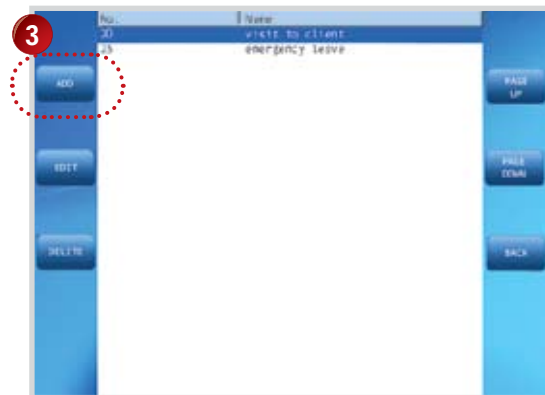
Select Add.

Enter a number to define the work code using numeric keypad, for example 30. Select Name field.
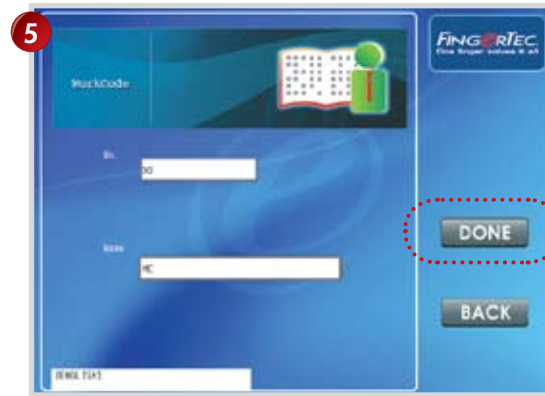
Enter the name of the work code by using T9 input method, for example MC. Select Done to save settings.
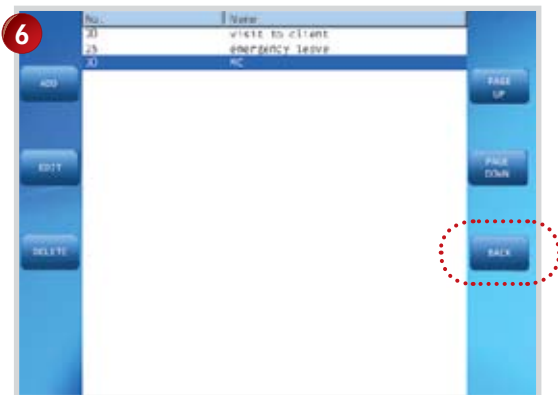
The screen will refresh and a new work code will be created.
Select Back to return to the previous page.

Select return arrow to go back to the main menu.

REMARK:
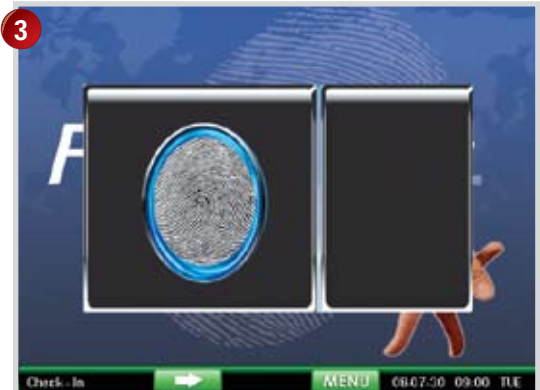It is recommended to define and upload work codes in
TCMS V2 software

TO ENTER WORK CODE DURING VERIFICATION

Input work code after verification: Select the asterisk (*) button.
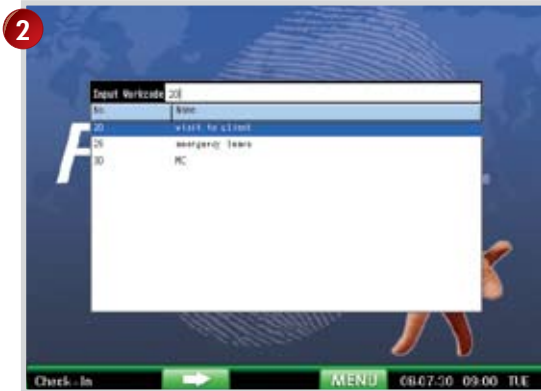
Enter the work code using the numeric keypad. Please make sure that the work code you enter is displayed on the screen. Select OK to proceed.

Place the enrolled fingerprint on the fingerprint sensor.

Wait a second before removing the finger from the fingerprint sensor. The reader will verify that you are a user; display the user ID and prompt "Thank you".

If verification failed, the reader will prompt, "Please try again."

PRESET SCHEDULE BELLS (ALARM)

The reader offers 56 preset scheduled bells (alarm). This schedule is intended to alert users of the beginning and ending of working sessions. To use this function, the reader needs to be connected to a bell or to an alarm system.

Follow these steps to define scheduled bells:

Select the Menu button.

Select Alarm.

Select ▲▼ to select a schedule to define alarm, for example, Schedule 1.

Enter time to set the alarm into the Bell Hours fields.

Select ▼ to go to Music field, and and select ▶ to select the type of music.

Select ▼ to go to Time field to define snoozing repeat, for example 3 times.

Please ignore State field.
Select Done to save settings.
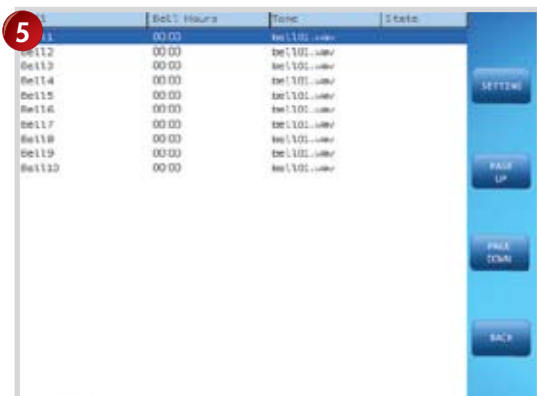
The screen will refresh and a new alarm time is defined.

Select to the return arrow to go back to the main menu.

BROADCAST
(SHORT MESSAGES DISPLAY)

The reader can display short messages on screen to alert users. There are 2 types of messages, public and personal. User can view the public messages all the time by pressing the asterisk (*) button. The personal messages are assigned to dedicated users only, and will be displayed only to the intended users after his/her verification. You can predefine the valid time period for the short messages from the onset of the display until its expiry period. The message will automatically be erased from the memory after the expiry period. While the short messages can be defined at the reader, it is strongly advisable to do it using the software. To do it via reader, follow the steps shown below:

Select the Menu button.

Select Broadcast.
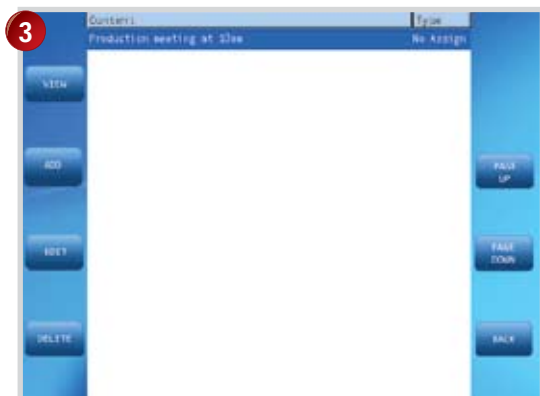
Select ▲▼ to choose the short messages for display.
Select Edit to proceed.
It is recommended to predefine the short messages using the software before uploading them to the reader.

Select ▲▼ to enter the start time of display.

Select ▼ to go to the Valid time field, for example 60 minutes.

Select ▼ go to the Type field to assign the messages as public or personal. messages.
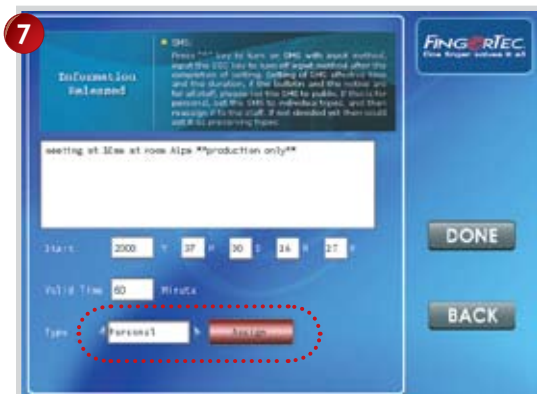
Press Done to save settings.
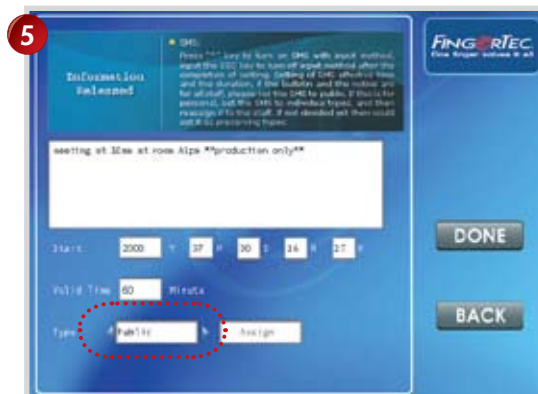
If the short message is assigned as Public, all users can view the message. Select Done to save settings.
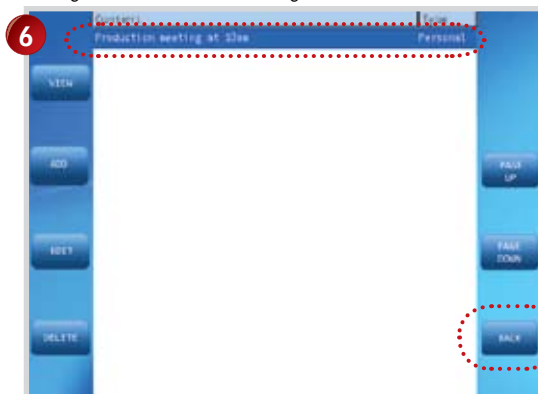
The page will refresh the content and type of the messahe.
Select Back to return to the previous page.

When the short message is assigned as Personal, only dedicated users can view it after verification.

Select ▶ to change message type to Personal.
Select Assign to proceed.

Press OK to dedicate the short messages to the users.
Press Done to save settings.
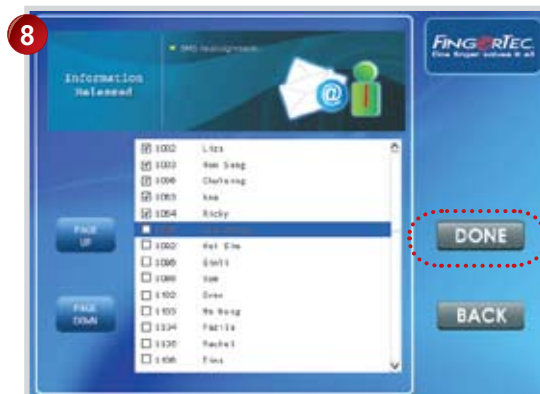
Select OK after choosing a recipient.
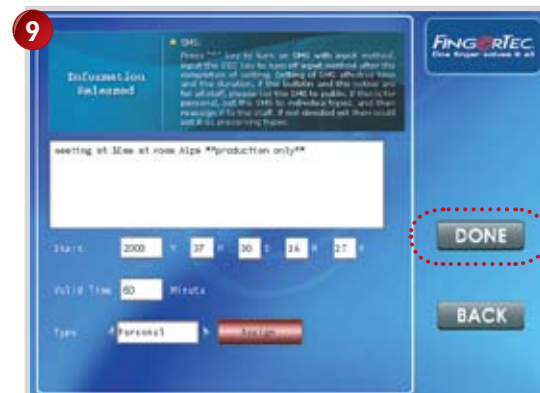
Select Done to save settings.
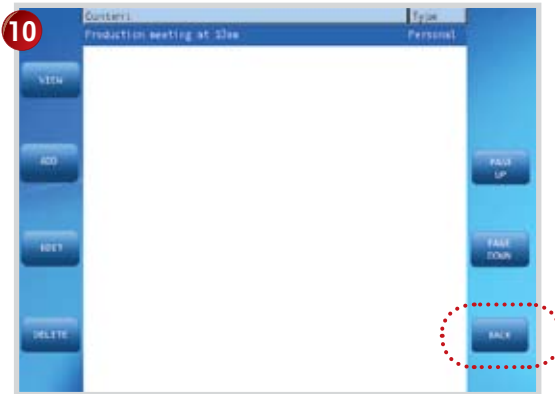
The screen will refresh and you can see the content and the type of the message.
Select Back to return to the previous page.

CAPTURE USERS PHOTO

The reader is integrated with a camera to capture user photo during verification. Every time a user verifies at the reader, the camera will capture the photo of the person. Administrator can choose to save or discard the captured photo. Refer to page (76) for more details.
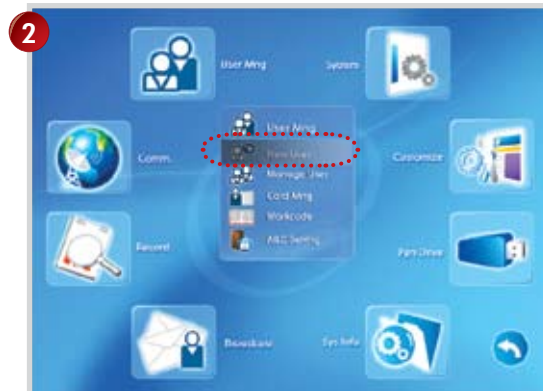
T9 INPUT METHOD

You can enter alphabet, symbols or numbers during configurations at the reader. You can use T9 input method to enter these information.

FOR EXAMPLE:
To input username by T9 input method:

Select Menu button.

Select New User.

Select ▼ go to the Name field.

Select asterisk (*) to input alphabet. Select 1 and a new line will be displayed at the bottom. Select 3 to select A.

Using similar steps, enter the name into the field.

The name is entered into the system.

6 SYSTEM OPTIONS

There are a total of 6 fields available in the system options.

PARAMETERS SETUP

Select System and choose Param Setup.

Threshold (1:1): To configure the sensitivity of the optical scanner during 1:1 matching. The threshold range is from 0 to 50; recommended threshold is 15.

(1:N): To configure the sensitivity of the optical scanner during 1 : N matching. The threshold range is from 0 to 50; recommended threshold is 35.

Date format: To change the display date format on screen.

Keybeep: To disable/enable the keypad sound

Voice: To disable/enable the greeting voice

Volume: To adjust the volume of the greeting voice, ranging from 0 to 100%. Recommended volume is 60%.

Log alert: To alert administrator when available space is less than the predefined value.

ReCheck Min: To configure reader to update any new transaction logs of user among a time period.

Space Alert: To alert administrator when the total space available is less than predefined value.

DATE/TIME ADJUSTMENT

Administrator can configure the reader to make the display date and time as local. It is important because the display date and time will affect the transaction logs of users.

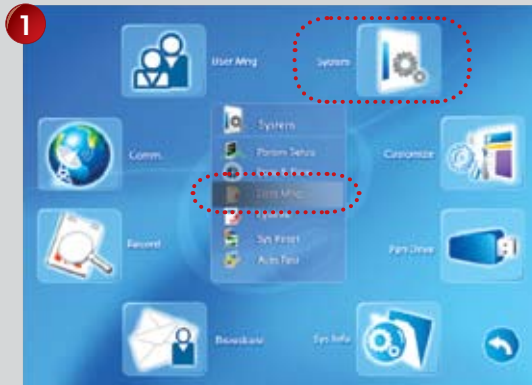Select System, followed by Date & Time.
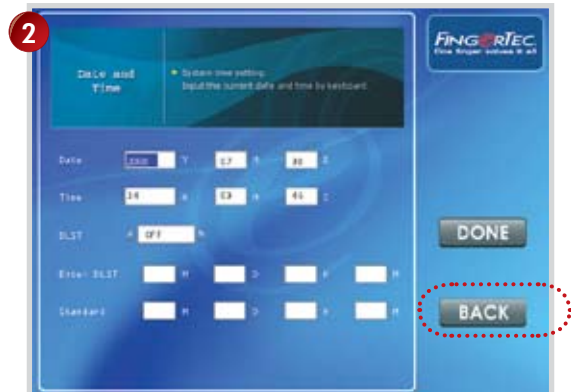
Select the ▲▼ to move to the corresponding field to enter the correct date and time.
Select Done to save settings.

DATA MANAGEMENT

As the data (user ID, names, fingerprint, password, Card ID, transaction logs etc) is stored inside the reader, the memory space is reduced during operation period. Therefore, it is recommended to clear the unnecessary data to maintain the reader working in perfect condition.

Select any of the options to clear specific data.

Select Back to return to the previous page after the process.

Delete Attlog: To delete all stored transaction logs.

Delete All: To delete all stored information.

Clear Authority: To clear administrator privilege.

**Delete pictures:** To delete pictures stored as wall paper

Delete capture-photo: To delete all photo captured after success verification.

Delete Black-List photo: To delete all photo captured after failed verification.

Select System followed by Data Mng.

UPDATE

This option is to allow installer to update the firmware version of the reader. The firmware is stored inside the USB flask disk and the disk has to be plugged into the reader. The update process will run automatically after the administrator select the Update button.
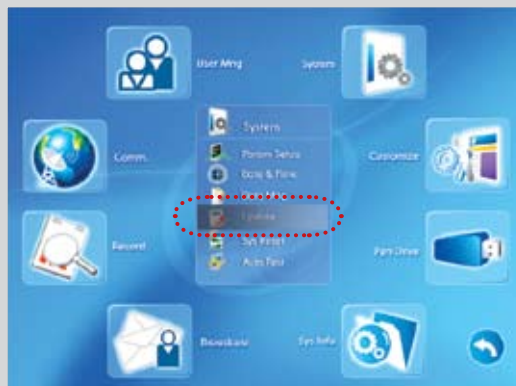
Plug the USB flash disk to the reader.
Select System followed by Update to start the update process.

SYSTEM RESET

This option is to reset all settings in the reader back to default. All data are kept during the reset process. It is not intended to clear storage of the reader but to reset settings to its default values.
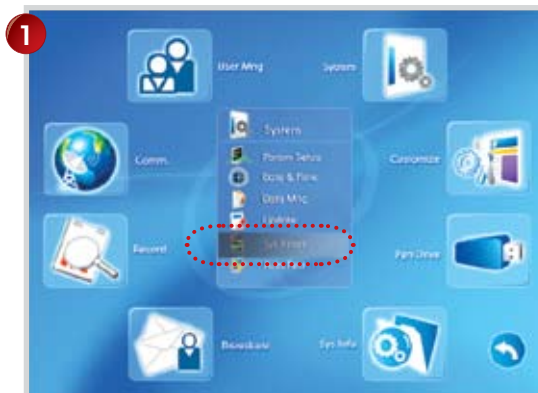
Plug the USB flash disk to the reader.

Select any of the options to reset specific settings.
Select Back to return to the previous page when done.

Reset all default parameters: To reset all settings in reader.

Reset keyboard parameters: To reset the shortcut keys on keyboard only.

Reset alarm parameters: To reset all time settings for alarms (scheduled bells).

Reset other parameters: To reset other parameters back to default settings.

AUTO TEST

This option is to allow installer to run testing on the reader to diagnose any error.
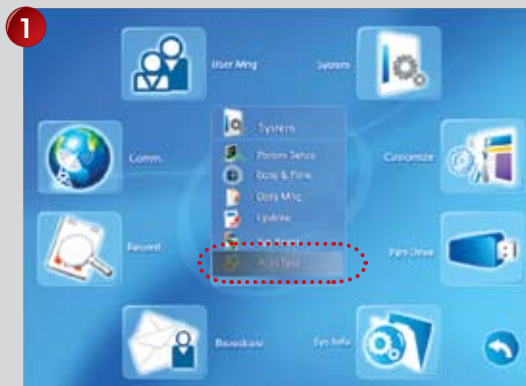
Select any of the options to run the specific test.

Select Back to return to previous page after done.

All Test: To run all test

TFT Test: To test the functionality of TFT screen.

Audio Test: To test the functionality of sound.

Keyboard Test: To test functionality of keyboard.

Sensor Test: To test the sensitivity of the optical scanner.

RTC Test: To test the accuracy of the real time clocking crystal.

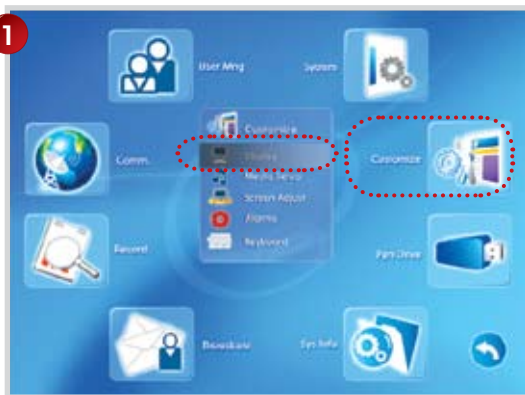# **7** **CUSTOMIZATION**

You can change the settings of reader to change its display screen, alarm outputs and keyboard input.

DISPLAY
This option will allow administrator to change the display settings on screen.

Select Customise followed by Display.

Select (arrow) to go to any field to change settings.
Select ◀▶ to adjust the value of each setting.
There are a total of 11 settings could be configured.

1:1 match retry times: To allow maximum number of tries for 1:1 fingerprint matching, ranging from 1 to 9, default as 3. If a user failed more than the allowed number, the reader will trigger alarm immediately. Ignore this function if your reader is not equipped with any alarm system.

Password retry times: To allow maximum number of tries during password verification. Range from 1 to 9, default as 3. If user fails more than the allowed trial, reader will trigger alarm immediately. Ignore if reader is not activate with any alarm system.

Clock mode: To select the display mode of clock on the screen during idle.

Picture delay: To define the delay time for picture to display on the screen during idle.

Clock delay: To define the delay time for clock to display on the screen during idle.

Sleep time: To define the time period for reader to go into sleep mode when it is idle. 0 value means that the reader will always be ON.

Adjust bright: To adjust the brightness of the display screen ranging from 0 to 100%. Default value is 70%.

FP image: To allow reader to display the captured fingerprint image. The image could be shown during verification, enrollment, or both. The image will not be shown if neither process is selected.

Standby Style: To configure reader to run music, flash and pictures during idle mode.

Lock Power: To disable the power On/Off button to prevent unauthorized switch off. The reader can only be shutdown by administrator when he/she access into this page.

Capture mode: To configure the image capture function in reader.

• *Capture only* – The reader will only capture user photo and display it on screen, but it will not be saved into the memory of the reader.

• *Capture and save* – The reader will capture user photo, display it on screen and save it into the memory of the reader.

MEDIA SETUP

This option is to adjust the settings of the integrated camera.

There are a total of 4 fields for camera adjustment.

Bright: To adjust the brightness of the camera ranging from 0 to 100%

Contrast: To adjust the contrast of the camera ranging from 0 to 100%.

Quality: To adjust the quality of capture image

Scene: To define the captured scene for outdoor or indoor.

Select Done to save settings.

Select Back to return to the previous page.

SCREEN ADJUST

This option is to allow installer to adjust the screen of the reader. Please always consult your local re-sellers or installer to do this for you.

ALARMS

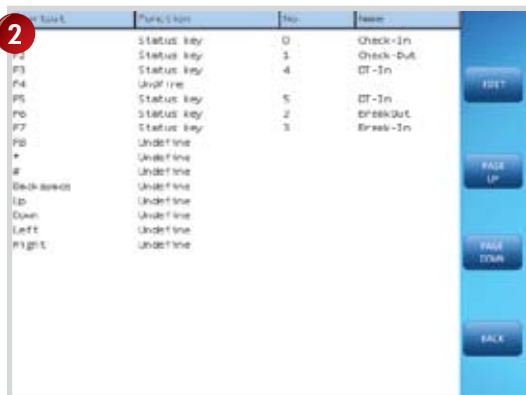This option is to configure the alarms or scheduled bells. Please refer page (61) for more details.

KEYBOARD

This option allows administrator to define shortcut keys for F1 to F8, asterisk (*), hash (#) etc.
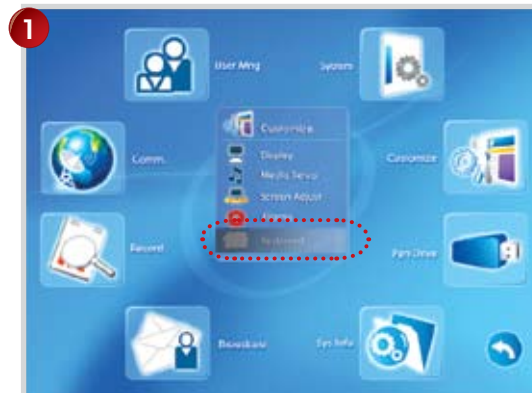
Select Customise followed by Keyboard.

Press ▲▼ to select button, which is to be defined with shortcut key.

Select Edit to define the shortcut key.

At the Function field, press ◄► to select the function for this shortcut key.

Select Done to save setting.

Select Back to return to the previous page.

8 RECORDS AND SYSTEM INFORMATION

RECORDS

Administrator can check user records at the reader. The transaction logs are in the form of raw clocking data with date and time. These records shall be used for reference only, for more detailed records and reports, please refer to the software.

To check these records:
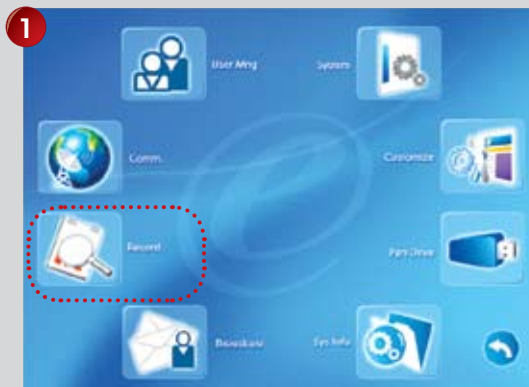
Select Records.

There are 3 options available to view specific records.

**Search Attlog:** To search and view user's transaction logs.

Search Capture-photo: To search and view photo captured after successful user verification.

Search Blacklist Photo: To search and view photo captured after a failed verification.

Select any of the function for example Search Attlog. Enter User ID to check with. Entering "All" means all users.

Enter User ID if you have a specific user ID. "All" is intended to search all users. Enter the starting and end date. Press Done to proceed.
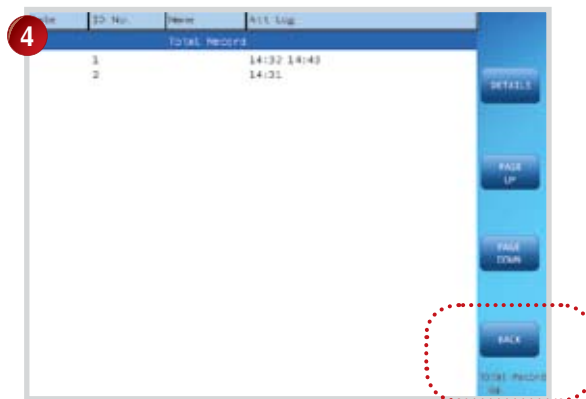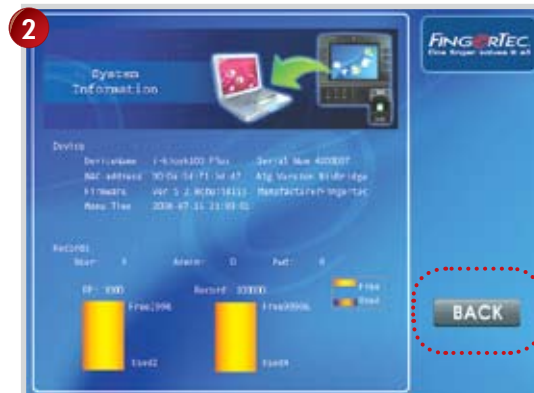

The search results will be displayed.
Press Back to return to the previous menu.

SYSTEM INFORMATION

Administrator can check the system information in the reader, for example total user enrolled, total transaction stored, space left, firmware version etc.

Press Sys Info to proceed.

All system information will be displayed on the screen.
Press Back to return to the previous menu.

9 INSTALLATION & COMMUNICATIONS

This Chapter is meant for qualified installer only. The installation of reader shall be handled by a well-trained installer. If you are not a qualified installer, you can ignore this Chapter or this Chapter serves as reference for all types of connections available for the reader only.

CONNECTION AVAILABLE

There is a lock protected the connection port of reader. Please make sure you have the key to unlock the connection port.
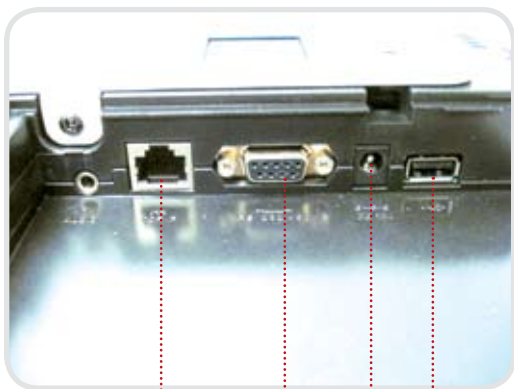
The locked connection port.

Unlock it by using the key comes together with the reader.

Pull the plastic protector to right side (as show by the arrow) to open it.

Please keep this key because it is unique for each reader.

TCP/IP port to provide TCP/IP communication to the computer via LAN cable.

USB port for data transferring.

DC12V power input to provide power to the reader.

Serial port to provide RS232 or RS485 communication to computer via RS232 or RS485 cable.

COMMUNICATIONS CONNECTION

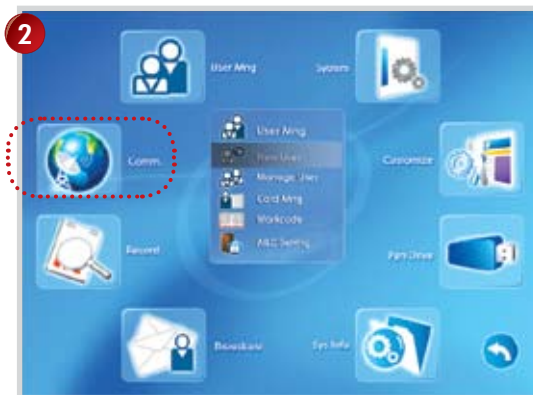The FingerTec® I-Kiosk 100 Plus can be connected to computer via 5 ways.

TCP/IP CONNECTION

Please follow the steps shown to configure to connect via TCP/IP.
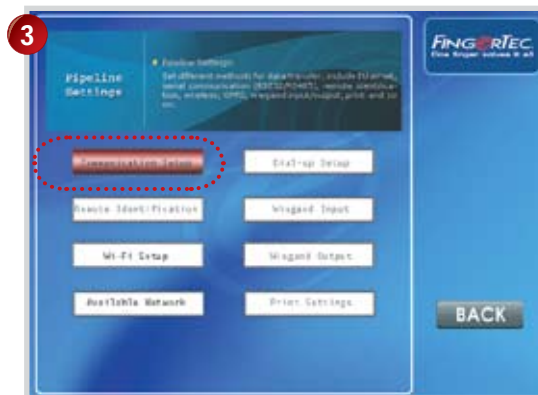

Press Menu button

Press COMM button.

Press Communication Setup.

Please enter the value by pressing keypad for these items,

IP address of the FingerTec® reader

Subnet Mask of the network environment.

Gateway of the network environment.

Netspeed of the network environment. Default as AUTO.

Device ID of the reader, default as 1.

Press Done to save settings

5

Press OK to confirm to save settings.

6 Return to the main menu.

7 Power off FingerTec® reader.

8 Plug in the LAN cable.

9 Power on the FingerTec® reader

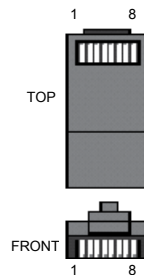*PC*

i-Kiosk 100 Plus Reader

Ethernet 10/100Base-T Crossover Cable

1   8

TOP

FRONT

1   8

This cable can be used to cascade hubs or for connecting two Ethernet stations back-to-back without a hub. It works with both 10Base-T and 100Base-TX.

Joint 1 Pin			Joint 2 Pin
TX+	1	3	RX+
TX-	2	6	RX-
RX+	3	1	TX+
RX-	6	2	TX-

Ethernet 10/100Base-T Straight Thru Cable

This cable will work with both 10Base-T and 100Base-TX and is used to connect a network interface card to a hub or network outlet. These cables are sometimes called "whips".

Connector Pin			Cable Color	Connector
TX+	1	White/Orange	1	TX+
TX-	2	Orange	2	TX-
RX+	3	White/Green	3	RX+
	4	Blue	4	
	5	White/Blue	5	
RX-	6	Green	6	RX-
	7	White/Brown	7	
	8	Brown	8	

RS232 CONNECTION

Please follow the steps shown to configure to connect via RS 232.

Press Menu button

i-Kiosk 100 Plus Reader   *RS232 Cable*   *PC*

Press COMM button.

Press Communication Setup.

Please enter the value by pressing keypad for these items,

Baudrates of RS232 connection, default as 115200.

RS 232 is turn ON.

RS 485 is turn OFF.

Device ID of the reader defaults as 1.

Press Done to save settings.

Press OK to confirm to save settings.

6 Return to the main menu.

7 Power off FingerTec® reader.

8 Plug in the RS232 cable.

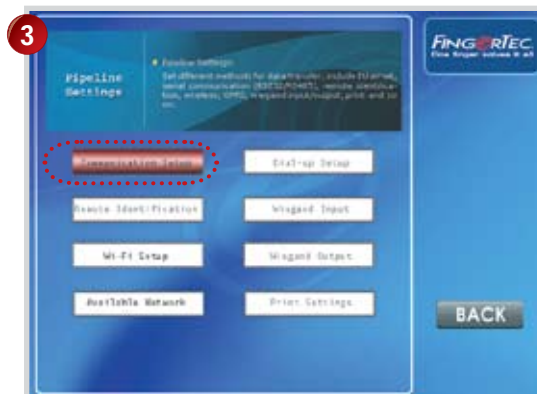**9** Power on the FingerTec® reader.

RS485 CONNECTION
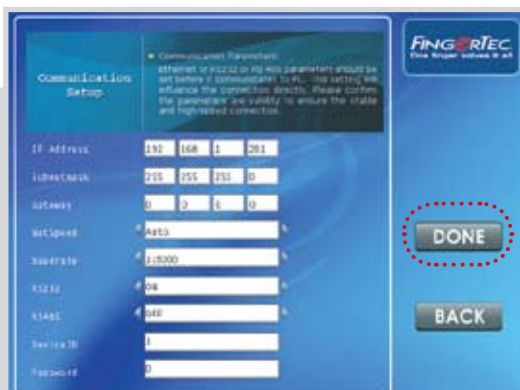Please follow the steps shown to configure to connect via RS485.

Press Menu button

Press COMM button.

Press Communication Setup.

Please enter the value by pressing keypad for these items,

Baudrates of RS232 connection, default as 115200.

RS 232 is turn OFF.

RS 485 is turn ON.

Device ID of the reader defaults as 1.
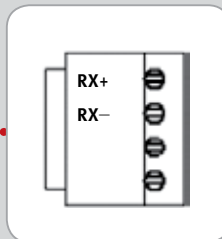
Press Done to save settings.

Press OK to confirm to save settings.

6 Return to the main menu.

7 Power off FingerTec® reader.

8 Plug in the RS232 cable to reader and RS232/485 data converter.

9 Power on the FingerTec® reader.

RS232/RS485 SINGLE CONNVERTER

RX+
RX−

i-Kiosk 100 Plus Reader   *RS232/RS485 Data Connverter*   *RS232 Cable*   *PC*
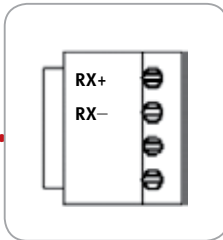
RS232/RS485 NETWORK CONNVERTER

i-Kiosk 100 Plus Reader   *RS232/RS485 Data Connverter*   *RS232 Cable*   *PC*
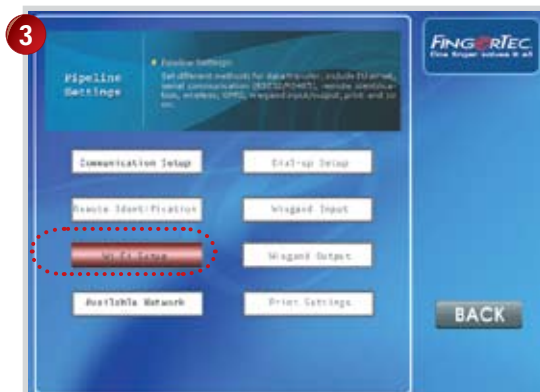
WIRELESS CONNECTION

Follow steps to configure reader to connect via wireless connection (WiFi).

Press Menu button.

Press COMM button.

Press WiFi Setup.

Enter the value of the WiFi rouner.
Press Done to save settings.

Press OK to confirm.

6 Return to the main menu.

7 Power off FingerTec® reader.
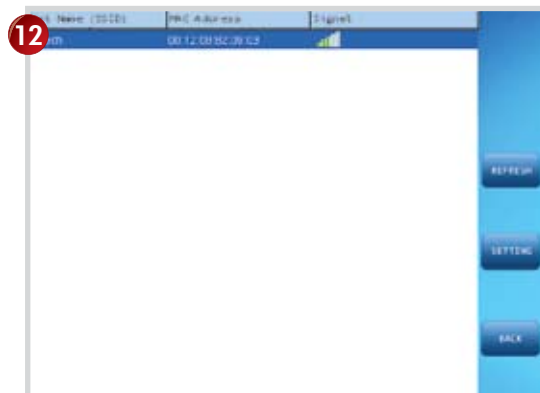
8 Power on the FingerTec® reader.

Press Menu button

Press COMM.

Press Available network.

The WiFi connection is showed when it is connected.

APPENDIX ● TROUBLESHOOTING

1 How to power on and shut down the FingerTec® i-Kiosk 100?

To power on, press the ON/OFF button once. To shut down, press and hold the ON/OFF button for 3 second.

2 I cannot connect the FingerTec® reader to the PC. Every time I try, the software prompts "Unable to connect" message. What should I do?

Please check communication settings in Menu > Option > Comm. Opt. Please see more details in page 46, Connection to Computer.

3 The FingerTec® reader has difficulty recognizing my fingerprint. It takes many tries before I am verified. What should I do?

Please make sure that your finger is not too oily or too dirty because the oil and dirt will cover the minutiae points of the fingerprints, thus making reading difficult. Make sure the FingerTec® reader is not facing direct sunlight because it will disturb the reading of the sensor. To deal with light interference, cover the reading area when you want to verify your fingerprint. If this occurred often, kindly ask for re-registration.

4 Alarm goes off every time when I place finger on the sensor. Why did such thing occur and what should I do?

The finger you used was defined as a duress finger. Once a duress finger is verified, it will trigger the FingerTec® reader to activate the alarm. To undefine your finger as a duress finger, follow these steps: Menu > Option > Access options > Duress Option > Duress FP > Undef Duress FP > Enter your user ID

5 When the FingerTec® reader is turned on, the red LED is blinking all the time. Is there any problem with the reader?

There is nothing wrong with the FingerTec® reader. The red LED blinks to indicate FingerTec® reader is on standby. When a fingerprint is verified, the LED will turn green to indicate successful verification.

6 The FingerTec® reader is accidentally turned off by a staff. Would we lose all the transaction data and fingerprints in that FingerTec® reader?

All transaction data and fingerprints in the FingerTec® reader is safe in the event of power shutdown because all the information is stored in the memory of the reader. This information can only be deleted via software or it can be manually purged in Advance option.

7 How to define the short message and assign it to certain users?

Refer to page 63-67 for instructions to define short messages. The easier way to define the short message is by using TCMS V2 software.

8 Do I need to clear the unwanted or outdated short messages in the reader?

Not necessary, as those messages will be deleted automatically after the predefined time period has expired.

9 During enrollment I heard "duplicate finger". Why was that?

The "duplicate finger" voice message is to alert user if the enrolling finger is found to have existed in the FingerTec® reader. User must use other finger to enroll.

10 I waved my RFID card to a FingerTec® reader but it did not respond. What could be the reason?

Please make sure that your RFID card is registered to the FingerTec® reader, before you use it. Please also make sure that your user ID is assigned into the verification group that supports RFID card.

11 Do I need to stop the USB pen drive like we usually do when used in computer before we could unplug it from the reader?

Not necessary because once download or upload operation is completed, it is safe for you to remove the USB pen drive from the reader.

www.fingertec.com